

**CLAIMS:**

1. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:
- (a) receiving a new alert;
  - (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
  - (c) updating a minimum similarity requirement for one or more features;
  - (d) updating a similarity expectation for one or more features;
  - (e) comparing the new alert with one or more alert classes, and either:
    - (f1) associating the new alert with the existing alert class that the new alert most closely matches; or
    - (f2) defining a new alert class that is associated with the new alert.
2. The method of claim 1 further comprising the step (a1) of passing each existing alert class through a transition model to generate a new prior belief state for each alert class.
3. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:
- (a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
  - (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
  - (c) comparing the new alert to one or more alert classes;
  - (d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value;
  - (e) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
    - (f1) associating the new alert with the existing alert class that the new alert most closely matches; or
    - (f2) defining a new alert class that is associated with the new alert.

4. In an intrusion detection system that includes a plurality of sensors, each of which generates alerts when attacks or anomalous incidents are detected, a method for organizing the alerts comprising the steps of:

- (a) receiving an alert;
- (b) identifying a set of features that may be shared by the received alert and one or more existing alert classes;
- (c) setting a minimum similarity value for one or more features or feature groups; comparing the new alert to one or more of the alert classes, and either:
  - (d1) defining a new alert class that is associated with the received alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value; or
  - (d2) associating the received alert with the existing alert class that the received alert most closely matches.

5. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:

- (a) receiving a new alert;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
- (c) updating a minimum similarity requirement for one or more features;
- (d) comparing the new alert with one or more alert classes, and either:
  - (e1) associating the new alert with the existing alert class that the new alert most closely matches; or
  - (e2) defining a new alert class that is associated with the new alert.

6. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

- (a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
- (c) comparing the new alert to one or more alert classes;

8 (d) rejecting a match if any feature for which a minimum similarity value has  
9 been set fails to meet or exceed the minimum similarity value, and either:

10 (e1) associating the new alert with the existing alert class that the new alert most  
11 closely matches; or

12 (e2) defining a new alert class that is associated with the new alert.